

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Primož Ivančič

Gostovanje uporabniških profilov

DIPLOMSKO DELO
VISOKOŠOLSKI STROKOVNI ŠTUDIJSKI PROGRAM PRVE STOPNJE
RAČUNALNIŠTVO IN INFORMATIKA

prof. dr. Miha Mraz
MENTOR

Ljubljana, 2014

© 2014, Univerza v Ljubljani, Fakulteta za računalništvo in informatiko

Rezultati diplomskega dela so intelektualna lastnina Fakultete za računalništvo in informatiko Univerze v Ljubljani. Za objavljanje ali izkoriščanje rezultatov diplomskega dela je potrebno pisno soglasje Fakultete za računalništvo in informatiko ter mentorja.¹

¹V dogovoru z mentorjem lahko kandidat diplomsko delo s pripadajočo izvirno kodo izda tudi pod katero izmed alternativnih licenc, ki ponuja določen del pravic vsem: npr. Creative Commons, GNU GPL.

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

Kandidat naj v svojem delu razišče tehnične rešitve za realizacijo gostovanja uporabniških profilov v okenskem okolju proizvajalca Microsoft. V domeni uporabnika profila naj kandidat definira osnovne uporabniške zahteve, realizira različne načine realizacije gostovanja profila, izvede oceno ustreznosti različnih tehničnih rešitev in izvede zmogljivostno analizo različnih rešitev z vidika hitrosti dostopanja do profilov z različnih lokacij.

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Spodaj podpisani Primož Ivančič, z vpisno številko **63990214**, sem avtor dela z naslovom:

Gostovanje uporabniških profilov

S svojim podpisom zagotavljam, da:

- sem delo izdelal samostojno pod mentorstvom prof. dr. Mihe Mraza,
- so elektronska oblika dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko in
- soglašam z javno objavo elektronske oblike dela v zbirki "Dela FRI".

V Ljubljani, dne 3. junija 2014

Podpis avtorja:

KAZALO

| | |
|---|------------|
| Povzetek | iii |
| Abstract | v |
| 1 Uvod | 1 |
| 2 Predstavitev problema | 3 |
| 2.1 Opis arhitekture sistema | 3 |
| 2.2 Vloga uporabnika v sistemu | 6 |
| 3 Uporabniški profili v okolju Microsoft Windows 7 | 9 |
| 3.1 Panj registrov | 10 |
| 3.2 Skupek map | 11 |
| 4 Predstavitev rešitev | 13 |
| 4.1 Opis virtualnega testnega okolja | 13 |
| 4.2 Ročno kopiranje uporabniških profilov | 15 |
| 4.3 Uporaba gostujočih profilov | 17 |
| 4.4 Uporaba preusmeritev map | 23 |
| 4.5 Uporaba gostujočih profilov s preusmerjenimi mapami | 28 |
| 4.6 Primerjava in problemi rešitev | 31 |
| 5 Sklepne ugotovitve | 35 |

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Primož Ivančič
Gostovanje uporabniških profilov

POVZETEK

V podjetju, kjer zaposleni uporabljajo najbolj razširjen operacijski sistem Microsoft Windows in obstaja potreba po delu na različnih delovnih postajah, je več kot zaželeno, da uporabnike na vsaki delovni postaji pričakajo datoteke in delovno okolje, kot so si ga prilagodili po svojih potrebah. Predstavili smo nekaj rešitev, ki na različne načine to omogočajo. V skladu z omejitvami in zahtevami podjetja smo se v pričujočem diplomskem delu omejili zgolj na Microsoftove rešitve. Na praktičnem primeru smo v virtualnem okolju preverili ustreznost rešitev gostujočih profilov in preusmerjenih map, ter kombinacijo obeh skupaj za uporabo v podjetju.

Ključne besede: gostujoči profili, preusmerjene mape, Microsoft Windows

University of Ljubljana
Faculty of Computer and Information Science

Primož Ivančič

Roaming user profiles

ABSTRACT

In company where employees use the most popular Microsoft Windows operating system, they need to work on different machines and it is more than desirable that users are able to use their own files and working environment as they customized them by their needs. We have presented solutions that make this possible in different ways. In accordance with the restrictions and requirements of the business we are in the present thesis limited only to Microsoft solutions. On a practical example in a virtual environment we examined the solution of roaming profiles and folder redirection and the combination of the two together for use in the company.

Key words: roaming profiles, folder redirection, Microsoft Windows

1 Uvod

V pričujočem diplomskem delu predstavljamo problem hitro rastoče bančne institucije z več sto zaposlenimi, ki pri svojem delu uporabljajo delovne postaje z operacijskim sistemom Windows, povezane s centralno lokacijo v Ljubljani. Uporabniki so v preteklosti opravljali svoje delo vsak na svoji delovni postaji, kasneje pa se je zaradi naglega večanja obsega poslovanja, odpiranja novih poslovalnic, odsotnosti in nadomeščanja pojavila potreba po dnevni selitvi uporabnikov. Problem je nastal takoj, ko se je uporabnik prijavil na drugo delovno postajo, saj ni imel dostopa do svojih dokumentov, namizja, internetnih bližnjic in digitalnih potrdil. Pred pričetkom dela je uporabnik poklical sistemskega administratorja, ki je moral najprej ugotoviti, kateri računalnik je uporabnik prej uporabljal. Postopek je bil lahko precej zamuden, saj uporabnik ni vedno vedel na katerem računalniku je delal, pogosto je bil računalnik ugasnjen in ga je moral nekdo prižgati, kopiranje datotek je bilo zamudno in je obremenjevalo mrežno povezavo. V primeru začasnega izpada mrežne povezave kopiranje sploh ni bilo možno. Namesto da bi bil problem s tem rešen, je nastalo še več novih. V primeru, da se je uporabnik vrnil na prejšnje delovno mesto, ni imel datotek, ki jih je spremenil ali ustvaril na začasnem

delovnem mestu. Če se je preselil večkrat, se je izgubila sled in kmalu se ni več vedelo iz katerega računalnika je potrebno kopirati njegove dokumente in katera je njihova zadnja verzija. Tako je prihajalo do izgub podatkov in slabe volje. Z naraščanjem števila uporabnikov je bilo težav vse več in potrebno je bilo najti rešitev, ki bi zagotavljala nemoteno delo ob prijavi na katerikoli računalnik brez intervencije sistemskega administratorja ter tveganja za izgubo podatkov.

V diplomskem delu bomo predstavili različne rešitve za omenjeni problem, opisali njihovo delovanje, primerjali prednosti in slabosti ter na podlagi kriterijev izbrali najustreznejšo rešitev za podjetje. V drugem poglavju bomo za lažje razumevanje problema na kratko predstavili informacijski sistem podjetja. V tretjem poglavju bomo opisali zgradbo uporabniškega profila v okolju Microsoft Windows 7, katerega poznavanje je potrebno za razumevanje rešitev opisanih v nadaljevanju. Četrto poglavje vsebuje teoretični opis rešitev in praktični preizkus tistih, ki izpolnjujejo zastavljene kriterije. V petem poglavju smo povzeli teoretične in praktične ugotovitve ter jih strnili v zaključek. Na koncu so navedeni viri, ki smo jih uporabili pri izdelavi diplomske naloge.

2 Predstavitev problema

Za potrebe opisa problema zagotavljanja enakega uporabnikovega delovnega okolja na vseh delovnih postajah v Delavski hranilnici d.d. Ljubljana je v prvem podpoglavju [2.1](#) na kratko predstavljen tisti del arhitekture informacijskega sistema podjetja, ki je ključnega pomena za predstavitev problema. Sledi podpoglavje [2.2](#), v katerem je predstavljena vloga posameznega uporabnika v sistemu. V nadaljevanju je na osnovi opisa arhitekture sistema in vloge posameznega uporabnika postavljena zahteva po implementaciji ustrezne tehnične rešitve, ki bi uporabnikom omogočala nemoteno delo na različnih delovnih postajah. Navedenih je nekaj tehnično različnih rešitev, na koncu pa je na podlagi zahtev izbrana najbolj ustrezna.

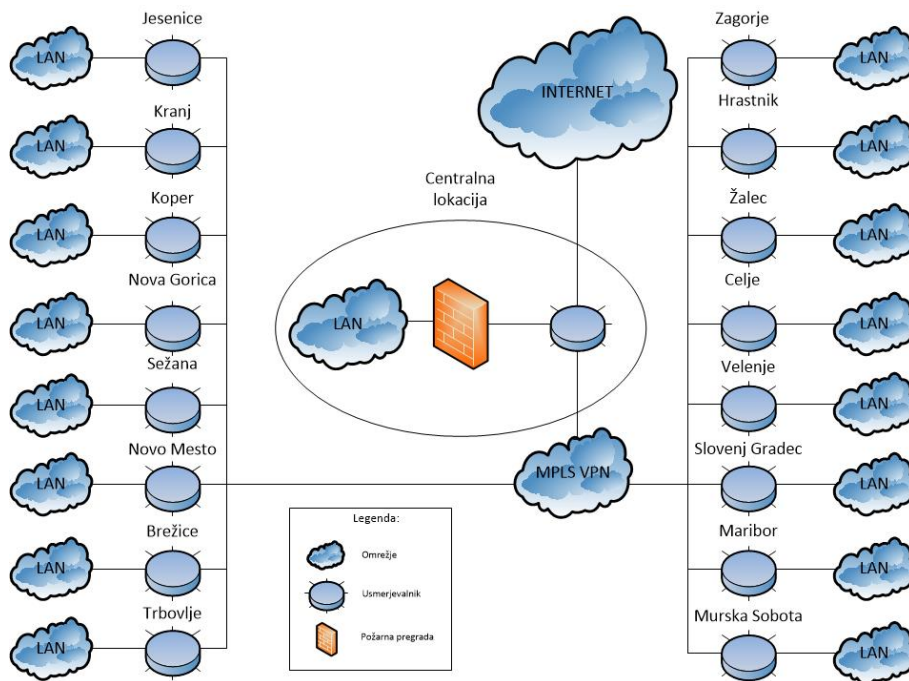
2.1 Opis arhitekture sistema

Informacijski sistem podjetja je zasnovan na principu odjemalec/strežnik, pri čemer so vsi uporabniki v vlogi odjemalca. Zaposleni uporabljajo delovne postaje, ki se nahajajo na centralni lokaciji v istem omrežju kot strežniki in na ločenih omrežjih v poslovalnicah. Delovne postaje v poslovalnicah so s centralno lokacijo povezane prek navideznega zaseb-

nega omrežja (VPN - *virtual private network*) in komunikacijske opreme, kot je prikazano na sliki 2.1. Centralno lokacijo tvori več strežnikov, požarna pregrada in tračna enota za izvajanje varnostnih kopij. Za lažjo predstavo je poenostavljena shema centralne lokacije s povezavo do ene izmed poslovalnic prikazana na sliki 2.2. Dva strežnika, produkcijski in rezervni, sta namenjena delovanju bančne aplikacije z Oracle bazo podatkov, do katere uporabniki dostopajo s spletnim brskalnikom. Preostali trije služijo za virtualizacijo informacijskega okolja in so povezani v gručo s produktom VMware vCenter Server 5. Na njih gostujejo sledeči virtualni strežniki:

- dva domenska strežnika Microsoft Windows Server Standard 2008R2 SP1, ki zagotavljata naslednje storitve:
 - storitve aktivnega imenika (AD - *active directory*);
 - zagotavljanje infrastrukture za skupinske politike (GPI - *group policy infrastructure*);
 - pomnjenje tabel za preslikave imen v IP naslove (DNS - *domain name system*);
 - dinamično dodeljevanje IP naslovov (DHCP - *dynamic host configuration protocol*);
- strežnik za elektronsko pošto Microsoft Windows Server Standard 2008R2 SP1, na katerem teče Microsoft Exchange Server 2010;
- strežnik za interno spletno stran Microsoft Windows Server Standard 2008R2 SP1, na katerem teče Microsoft Share Point 2010;
- strežnik za IP telefonijo Linux Suse, na katerem teče namenska aplikacija;
- strežnik za kontrolo pristopa Server Standard 2008R2 SP1, na katerem teče namenska aplikacija;

Tračna enota služi za zapis varnostnih kopij podatkov bančne aplikacije in posameznih strežnikov na kasete, kamor se shranjujejo samo podatki, ki se nahajajo na centralni lokaciji. Zapis podatkov iz delovnih postaj je tehnično možen, vendar bi morale biti v času izvajanja varnostnih kopij prižgane, uporabniki pa ne bi smeli imeti odprtih dokumentov. Zapis na trakove se izvaja zaporedno, kar pomeni da bi se kopiranje vršilo iz vsake postaje posebej in ne iz vseh naenkrat. Zaradi števila delovnih postaj in hitrosti povezave bi vsako kopiranje trajalo več dni. Na centralni lokaciji je v uporabi več kot 60, v 27 poslovnih enotah, ki se nahajajo v različnih slovenskih mestih, pa po 2 do 11 delovnih postaj, ki imajo nameščeno naslednjo programsko opremo:

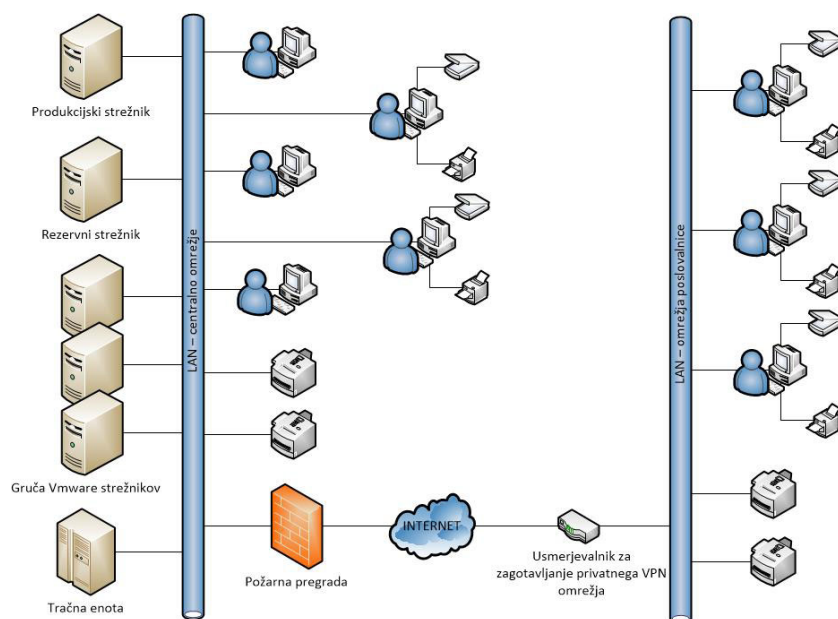


Slika 2.1 Shema omrežja, ki prikazuje povezave poslovalnic s centralno lokacijo.

- operacijski sistem Windows 7 SP1;
- pisarniški paket Microsoft Office 2010;
- spletni brskalnik Microsoft Internet Explorer 10;

Vse delovne postaje so pridružene v domeno. Nad njimi se z uporabo objektov skupinske politike (GPO - *group policy object*) izvajajo posamezne skupinske politike (GP - *group policy*), ki poskrbijo za izvajanje pravil, kot npr.:

- nadzor nad uporabniškim računom: veljavnost gesla npr. 30 dni, kompleksnost gesla, maksimalno število napačnih vnosov gesla;
- ohranjevalnik zaslona, ki se vključi po 7 minutah neaktivnosti, izključi pa z vnosom gesla, uporabnik nima možnosti spreminjanja te nastavitve;
- na namizju bližnjica do uporabnikovih dokumentov, ki se nahajajo na trdem disku delovne postaje;
- na namizju bližnjice do programov pisarniškega paketa Microsoft Office ter portala za dostop do namenske aplikacije;
- v spletnem brskalniku je kot privzeta nastavljena interna spletna stran, uporabnik tega ne more spremeniti;



Slika 2.2 Arhitektura informacijskega sistema: na levi strani je prikazana centralna lokacija s strežniki in delovnimi postajami, na desni pa fizično ločena enota z delovnimi postajami, ki imajo dostop do strežnikov prek optične povezave z uporabo navideznega zasebnega omrežja.

- onemogočeno pisanje na prenosne medije (USB, CD-ROM);
- sprememba nastavitve sistemskih popravkov operacijskega sistema Windows v skladu s politiko podjetja;

2.2 Vloga uporabnika v sistemu

Delovne postaje imajo dostop do več različnih mrežnih tiskalnikov na isti lokaciji, ti-
ste, ki so namenjene bančnemu poslovanju pa imajo priključen optični čitalec za branje
univerzalnih plačilnih nalogov in poseben namenski tiskalnik za potrjevanje nalogov ter
tiskanje na listke za vplačilo in izplačilo. Delovni proces poteka tako, da se uporabnik
ob pričetku dela s svojim uporabniškim imenom in geslom prijavi na eno izmed delovnih
postaj. Zažene bančno aplikacijo ter izvršuje bančne storitve. Do podatkov potrebnih za
delo dostopa prek bančne aplikacije, poleg tega pa uporablja pisarniška orodja Microsoft
Office Word in Excel s pomočjo katerih kreira, pregleduje in popravlja dokumente. S
programom Microsoft Outlook dostopa do svojega predala za elektronsko pošto, spletni
brskalnik pa uporablja za dostop do intraneta in interneta. Po končanem delu se upo-
rabnik odjavi. Na začetku poslovanja je imel vsak uporabnik svojo delovno postajo. Z

naglim širjenjem poslovanja se je pojavila potreba po seljenju uporabnikov med različnimi delovnimi postajami, tako znotraj centralne lokacije, kot tudi med posameznimi poslovalnicami. Za zagotavljanje nemotenega dela je zelo pomembno, da ima uporabnik na vsaki delovni postaji dostop do svojih dokumentov, ki so za primer okvare trdega diska arhivirani na trakove.

Potrebno je najti rešitev, ki jo je možno brez dodatnih stroškov implementirati na obstoječi infrastrukturi in izpolnjuje naslednje pogoje:

- omogoča vsem uporabnikom dostop do svojih dokumentov, namizja, internetnih bližnjic iz katerekoli delovne postaje;
- shranjuje uporabnikove podatke na centralnem strežniku, kjer je možno izdelati varnostne kopije na arhivske trakove;
- omogoča delo oz. dostop do podatkov v primeru začasnega izpada omrežne povezave;

Obstaja več tehnično različnih rešitev, s pomočjo katerih bi lahko delno ali v celoti rešili predstavljen problem. Nekaj primerov:

- uporaba uporabniških profilov, katerih prisotnost na delovnih postajah lahko zagotovimo na več načinov;
- uporaba prenosnih računalnikov, katere uporabniki selijo s seboj na različna delovna mesta;
- uporaba virtualne namizne infrastrukture, ki uporabnikom iz katerekoli delovne postaje omogoča dostop do lastne virtualne delovne postaje;

Za izpolnitev postavljenih pogojev najbolj ustreza uporaba uporabniških profilov, saj je edina od navedenih, ki jo je možno uporabiti brez nakupa dodatne strojne in programske opreme. Zato bomo v nadaljevanju bolj podrobno predstavili različice rešitve, ki zagotavlja prisotnost profilov na različnih delovnih postajah v podjetju.

3 Uporabniški profili v okolju Microsoft Windows 7

V okolju Microsoft Windows 7 so nastavitve delovnega okolja in podatki uporabnikov shranjeni v njihovih profilih. Za lažje razumevanje in reševanje problema, je potrebno pogledati zgradbo profilov.

Uporabniški profil [5] je zbirka nastavitvev, ki jo operacijski sistem kreira ob prvi prijavi uporabnika na delovno postajo. Ob vsaki naslednji prijavi operacijski sistem naloži uporabniški profil, ostale sistemske komponente pa nastavijo uporabniško okolje v skladu z informacijami v profilu. Ob vsaki prijavi je zagotovljeno, da uporabniško okolje izgleda in deluje tako, kot si uporabnik želi. Vsebuje uporabnikove dokumente, internetne bližnjice, piškotke, vsebino menija start, kot tudi regionalne nastavitve, ozadje namizja, ohranjevalnik zaslona, zvok, izgled kazalcev, aplikacij... Profil je tesno povezan z uporabniškim računom, ki služi za prijavo v operacijski sistem Windows in vsebuje informacije o pravicah za dostop do posameznih map in datotek ter dovoljenjih za izvajanje sprememb. Uporabniški profil je sestavljen iz dveh delov:

- "Registry hive": register je podatkovna baza v kateri so shranjene nastavitve, ki se nanašajo na uporabnika in računalnik. Del registrov se shrani v datoteko, ki ji

rečemo panj in se ob uporabnikovi prijavi naloži nazaj v registre. Registrski panj uporabniškega profila se nahaja v obliki datoteke NTUSER.DAT, ob prijavi pa se preslika na del registra HKEY_CURRENT_USER. Vsebuje nastavitve mrežne povezave, nadzorne plošče in nastavitve za posamezne aplikacije, ki so unikatne za uporabnika. Do večine nastavitvev uporabnik nima dostopa. Spreminjajo jih individualne aplikacije in komponente operacijskega sistema.

- Skupek map shranjen na lokalnem disku: datoteke uporabniškega profila se nahajajo v mapah z imenom uporabniškega računa, ki so v starejših različicah Windows shranjene v mapi Users in jim rečemo uporabniška mapa. Uporabniško mapo zapolnijo aplikacije in druge komponente operacijskega sistema s podmapami in uporabnikovimi podatki, kot so bližnjice, ikone namizja, aplikacije za hitri zagon, dokumenti, nastavitvene datoteke in tako dalje.

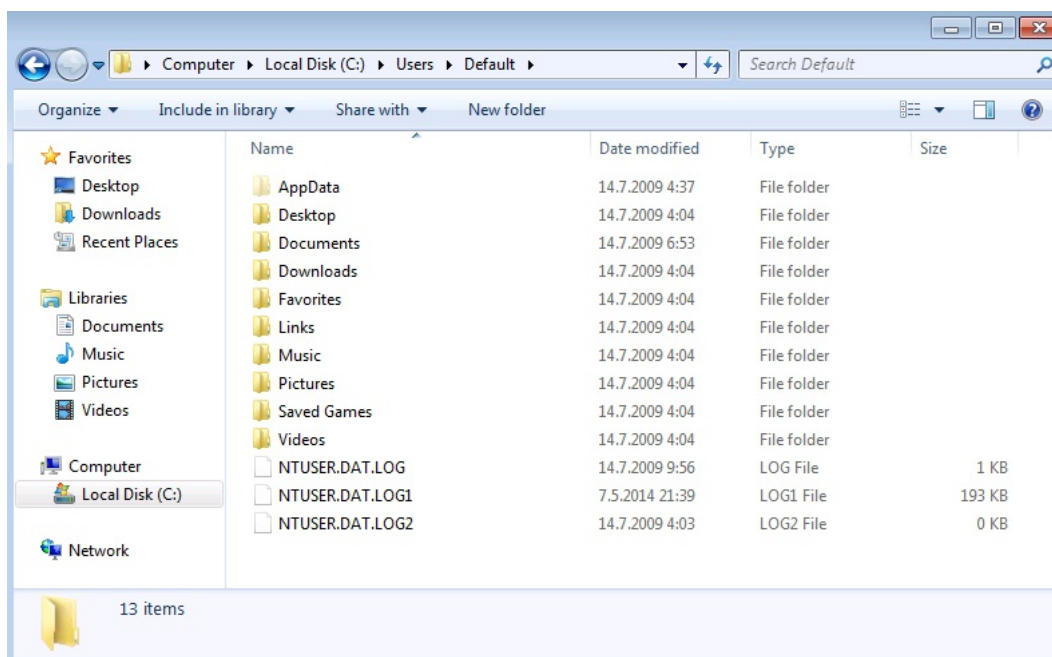
Obe komponenti skupaj tvorita uporabniške nastavitve, ki jih je možno migrirati med računalniki. Uporabniški profil zagotavlja naslednje prednosti:

- Sistem ob vsaki naslednji prijavi na delovno postajo zagotavlja enake nastavitve kot ob predhodnji prijavi.
- Če si delovno postajo deli več uporabnikov, ima vsak uporabnik svoje prilagojeno namizje.
- Nastavitve v uporabnikovem profilu so edinstvene za vsakega uporabnika. Drugi uporabniki do njih ne morejo dostopati. Sprememba v enem profilu ne vpliva na druge uporabnike ali na njihove profile.

3.1 Panj registrov

Panj registrov, ki je shranjen v datoteki NTUSER.DAT, vsebuje naslednje nastavitve:

- nastavitve Windows Raziskovalca, vse uporabniško definirane nastavitve za Windows raziskovalca in mrežne povezave;
- nastavitve opravilne vrstice;
- nastavitve tiskalnikov in povezave do omrežnih tiskalnikov;
- nadzorno ploščo in vse uporabniško definirane nastavitve v nadzorni plošči;
- pripomočke, vse uporabniške nastavitve za aplikacije, ki vplivajo na Windows okolje in vključujejo Računalo, Uro, Beležnico, Slikarja...;
- nastavitve aplikacij;



Slika 3.1 Prikaz datotečne strukture uporabniškega profila.

3.2 Skupek map

Mapo uporabniškega profila sestavlja več podmap, kot je razvidno s slike 3.1. Nekatere so uporabniku vidne in vsebujejo njegove datoteke, druge so sistemske, uporabniku skrite in so namenjene aplikacijam, shranjevanju sistemskih nastavitev in začasnim datotekam. Sistemska mapa uporabnikom ni vidna in AppData vsebuje naslednje podmape:

- Local: vsebina mape se ne nanaša na uporabnika ampak na računalnik;
- Roaming: mapa namenjena sinhronizaciji podatkov na strežnik v domenskih okoljih, kjer se uporablja roaming profile;
- LocalLow: mapa namenjena aplikacijam, za zapis začnih datotek na datotečni sistem;

Struktura uporabnikom vidnih map, ki vsebujejo njihove datoteke je sestavljena iz podmap:

- Desktop: mapa vsebuje datoteke prikazane na namizju;
- Documents: mapa namenjena uporabnikovim dokumentom; aplikacije naj bi vanjo privzeto shranjevale uporabnikove dokumente;

- Downloads: mapa namenjena shranjevanju datotek prenesenih s spleta;
- Favorites: mapa vsebuje zbirko internetnih bližnjic, ki so na voljo v brskalniku Internet Explorer;
- Links: mapa vsebuje zbirko bližnjic, prikazanih med bližnjicami v Windows Raziskovalcu;
- Music: mapa je namenjena za multimedijske avdio vsebine;
- Pictures: mapa je namenjena hrambi slik; aplikacije za delo s slikami naj bi jo privzeto uporabljale;
- Saved Games: mapa je namenjena shranjevanju podatkov igrice;
- Videos: mapa je namenjena multimedijskim video vsebinam.

Vsebina datoteke NTUSERS.DAT je opisana v podpoglavju 3.1. 'Panj registrov' in skupek map tvorita uporabniški profil, v katerem so shranjene nastavitve delovnega okolja in uporabnikove datoteke.

4 Predstavitev rešitev

V pričujočem poglavju bomo predstavili več različnih rešitev, ki uporabnikom omogočajo delo s svojim profilom na različnih delovnih postajah. Rešitve, ki so primerne za podjetje, bomo bolj podrobno predstavili, poiskali prednosti in slabosti ter delovanje preizkusili v testnem virtualnem okolju.

4.1 Opis virtualnega testnega okolja

Na delovni postaji s hitrim SSD (ang. *solid state disk*) in operacijskim sistemom Windows 8 smo za virtualizacijo uporabili Microsoftov Hyper-V. Namestili smo virtualni domenski strežniki Microsoft Windows Server 2008 R2 [2] z imenom **ad1** in dve virtualni delovni postaji z operacijskim sistemom Microsoft Windows 7, ki smo ju poimenovali **pc1** in **pc2** ter pridružili v domeno. Delovna postaja **pc1** bo služila kot primer delovne postaje na centralni lokaciji, zato hitrosti omrežja nismo omejevali, medtem ko bo delovna postaja **pc2** služila za simulacijo delovne postaje v poslovalnici, ki so v podjetju s centralno lokacijo povezane z optično povezavo s hitrostjo 5/5 Mbit/s. Pasovno širino mrežne povezave virtualne delovne postaje **pc2** smo zato omejili na 5 Mbit/s [9]. Za potrebe testiranja

smo za vsako rešitev kreirali drugega uporabnika. Zaradi primerljivosti rezultatov smo vsakemu izmed uporabnikov ob prvi prijavi na delovno postajo **pc1** nastavili enak profil. Nastavili smo:

- ozadje namizja: uporabili smo vnaprej pripravljeno sliko;
- ikone in bližnjice na namizju: prikaz 'My Computer', ustvarili smo bližnjico do 'Moji dokumenti', kreirali datoteko test.txt, ki je vsebovala niz znakov: '1,2,3,4,5', za testiranje spremembe vsebine datotek;
- orodna vrstica: odstranili smo bližnjico za 'media player' in nastavili bližnjici za 'WordPad' in 'Calculator';
- nastavitve programov: v programu 'Calculator' smo izbrali način 'Sceintific';

V mapi 'Moji dokumenti', smo s pomočjo prosto dostopnega programa File Generator [14] generirali 1100 naključnih uporabnikovih datotek, ki skupaj zasedejo 1,09 GB prostora na disku:

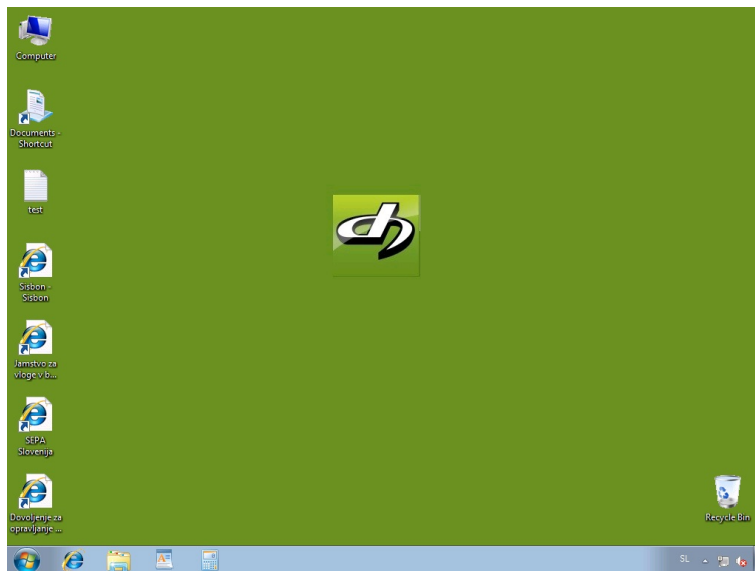
- 450 naključnih datotek velikosti 128 KB;
- 150 naključnih datotek velikosti 256 KB;
- 150 naključnih datotek velikosti 512 KB;
- 150 naključnih datotek velikosti 1024 KB;
- 150 naključnih datotek velikosti 2048 KB;
- 50 naključnih datotek velikosti 10240 KB;

Zagnali smo spletni brskalnik Internet Explorer, kjer smo:

- ob prvem zagonu potrdili privzete nastavitve,
- skrili prikaz 'Favorites Bar',
- za domačo stran nastavili stran Delavske hranilnice d.d.,
- dodali med priljubljene štiri strani in njihove bližnjice kopirali na namizje,
- dodali kvalificirano digitalno potrdilo.

Namizje vseh uporabnikov je pred odjavo iz delovne postaje **pc1** izgledalo tako, kot je prikazano na sliki 4.1. Pri preizkusu rešitev smo merili čas potreben za prijavo in odjavo:

- v primeru prijave: vnesli smo uporabniško ime in geslo, nato pa smo izmerili čas od pritiska na tipko za prijavo do popolnoma naloženega namizja;
- v primeru odjave: čas od klika na tipko za odjavo do prikaza zaslona za ponovno prijavo.



Slika 4.1 Izgled prilagojenega namizja uporabnika.

Medtem ko je bil uporabnik prijavljen, smo preverili nastavitve profila in podatke. Preverili smo tudi, če profil vsebuje spremembe, ki smo jih naredili pri predhodnji prijavi. V naslednjem podpoglavju bomo, kot prikaz selitve uporabnika v praksi, brez uporabe katera od ustrežnejših rešitev, opisali rešitev ročnega kopiranja, ki je iz praktičnih razlogov ne bomo preizkusili v virtualnem okolju. Sledeča tri poglavja so namenjena predstavitvi rešitev gostujočih profilov, preusmerjenih map in kombinacije obeh skupaj. V zadnjem podpoglavju bomo predstavili probleme, do katerih lahko pride v praksi pri uporabi gostujočih profilov v kombinaciji s preusmerjenimi mapami.

4.2 Ročno kopiranje uporabniških profilov

Rešitev v praksi zahteva posredovanje sistemskega administratorja ob vsaki selitvi uporabnika na drugo delovno postajo. Delovni proces je v tem času moten, trajanje pa je odvisno od hitrosti povezave ter količine in velikosti uporabnikovih datotek. Ob selitvi mora administrator vedeti, kateri računalnik je uporabnik prej uporabljal. Računalnik mora biti prižgan, administrator pa mora potem ročno pregledati mapo uporabniškega profila in kopirati vsebino map uporabnikovih dokumentov, namizja ter bližnjic za spletni brskalnik. Digitalnih potrdil na ta način ni mogoče kopirati. Za selitev potrdil je potrebna prijava uporabnika na računalnik, kjer se nahajajo in izvoz, kar pa ni vedno

možno, saj so digitalna potrdila lahko zaradi varnosti uvožena tako, da jih ni več mogoče izvoziti. Ko se uporabnik preseli nazaj na računalnik, kjer je delal prej, tam nima dokumentov in sprememb, ki jih je ustvaril na novem računalniku, zato je zopet potrebna intervencija administratorja. Najbolje je, če se na starem računalniku vsebine uporabnikove mape 'Moji dokumenti', namizja in bližnjic izbriše. Možno je, da je uporabnik na začasnem računalniku nekatere dokumente izbrisal in bi tako v primeru kopiranja celotne vsebine uporabnikove mape 'Moji dokumenti' ostale datoteke, ki jih uporabnik več ne potrebuje.

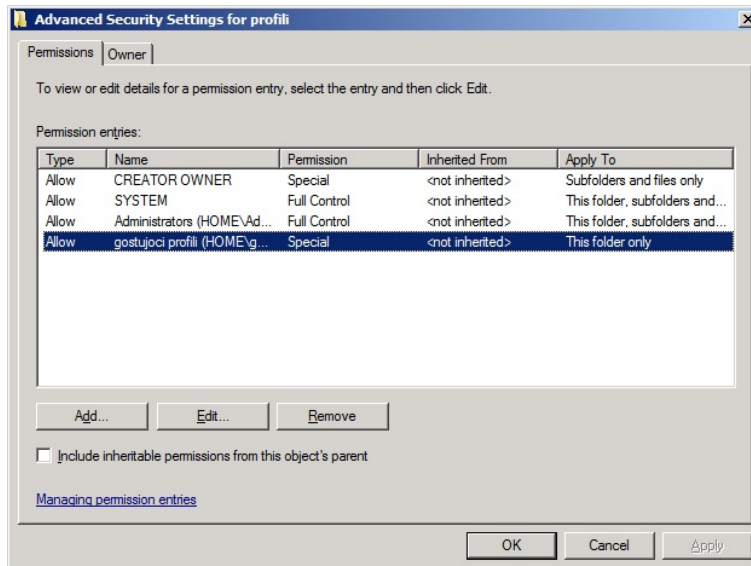
V primeru selitve na katerikoli računalnik je vedno potrebno vedeti, kje se nahaja zadnja verzija podatkov, kar pa ni vedno mogoče. V praksi se lahko zgodi, da se uporabnik prijavi na nek računalnik, kjer je sicer že gostoval in ima že od prej neko kopijo namizja in dokumentov, ki izgleda na prvi pogled zelo podobna. Ker ne opazi, da kopija ni aktualna, lahko prične z delom in prične s popravljanjem starih verzij datotek.

Tako se po določenem času zgodi, da je na mnogih računalnikih po omrežju množica profilov, ki med seboj niso sinhronizirani, nekateri vsebujejo stare dokumente, ki jih je uporabnik že izbrisal, drugi pa vsebujejo kakšnega novega. Po daljši uporabi in selitvi uporabnikov po vseh računalnikih v omrežju je izredno težko ugotoviti na katerih računalnikih je uporabnik sploh delal, še težje pa je poiskati ustrezne zadnje verzije posameznih dokumentov. Tako lahko pride do izgube pomembnih podatkov.

Problemom bi se lahko izognili, če profilov ne bi kopirali ampak premikali, vendar pa v tem primeru uporabnik po selitvi nazaj ne bi mogel takoj pričeti z delom, saj ne bi imel svojih dokumentov. Ročna rešitev je zamudna, zahteva precej časa in natančnosti, zaposli sistemskega administratorja in uporabnika ter prinaša obilico možnosti za izgubo podatkov in je primerna samo, če je število selitev minimalno. V primeru, da se na isti dan seli več uporabnikov, morajo počakati v vrsti, da sistemski administrator preseli vsakega posebej, preden lahko pričnejo z delom.

Rešitev za podjetje ni primerna, saj ne izpolnjuje treh pomembnih pogojev:

- ne omogoča uporabnikom dostopa do svojih dokumentov, namizja, internetnih bližnjic iz katerekoli delovne postaje brez zamudnega posredovanja;
- ne zagotavlja shranjevanja uporabniških profilov na centralnem strežniku, kjer jih je možno arhivirati na varnostne trakove;
- omogoča delo oz. dostop do podatkov v primeru začasnega izpada omrežne povezave, če je uporabnik že pred izpadom uporabljal to delovno postajo.

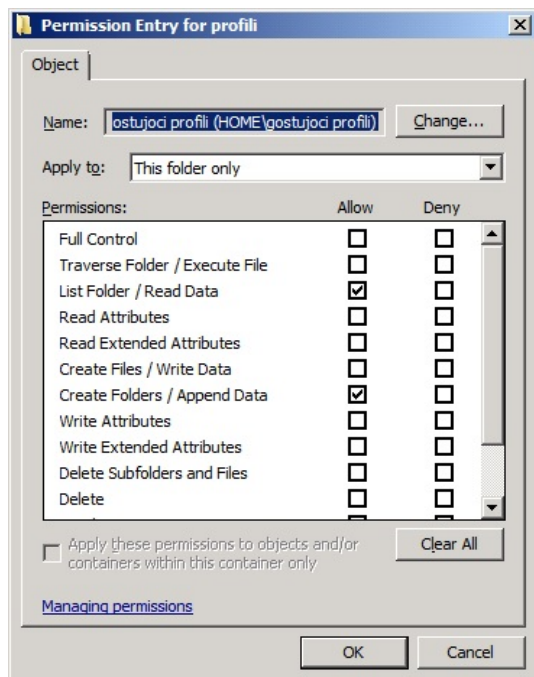


Slika 4.2 Izključeno dedovanje v varnostnih nastavitvah mape profili v naprednih varnostnih nastavitvah.

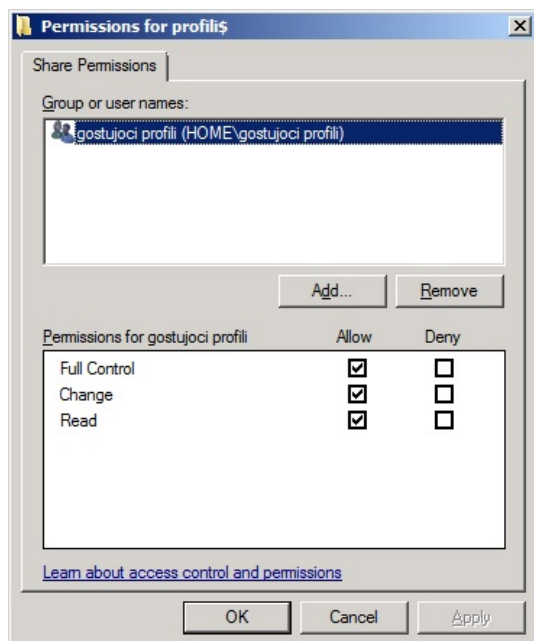
4.3 Uporaba gostujočih profilov

V Microsoftovem domenskem okolju je od verzije Microsoft Windows 2000 Server naprej omogočeno shranjevanje uporabniških profilov na strežnik. Take profile imenujemo gostujoči profili (ang. *roaming user profiles*) [6]. Microsoft je tehnologijo z vsako novejšo generacijo spremenil in izboljšal.

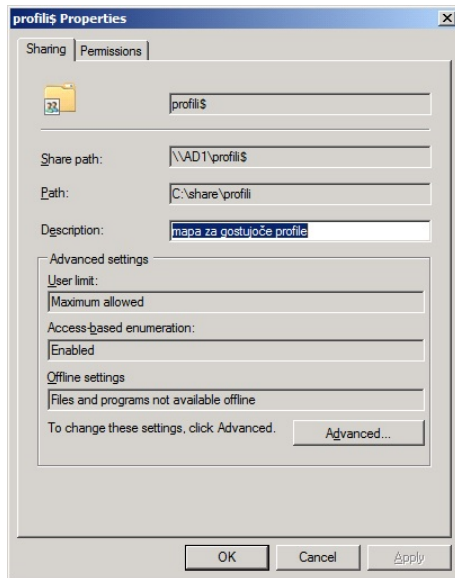
Za preizkus rešitve v testnem okolju smo na virtualnem domenskem strežniku **ad1** kreirali uporabnika z uporabniškim imenom **uporabnik1**, ter varnostno skupino *gostujoci profili*, ki jo bomo v skladu z dobro prakso potrebovali (ang. *best practice*) za nastavitve varnostnih pravic [8] in dodeljevanja skupne rabe. Shranjevanju datotek uporabniških profilov smo v virtualnem testnem okolju namenili kar domenski strežnik. Slednje ni v skladu z dobro prakso, ki za te namene priporoča ločen datotečni strežnik. Na trdem disku strežnika **ad1** smo kreirali mapo z imenom **profili**, ki bo služila za shranjevanje datotek uporabnikovega profila. V naprednih varnostnih nastavitvah smo izključili dedovanje varnostnih pravic, kot je prikazano na sliki 4.2. V nastavitvah dovoljenj smo skupini *gostujoci profili* dodali pravice za vpogled v seznam map (ang. *List Folder / Read Data*) in kreiranje novih map (ang. *Create Folders / Append Data*), kot je prikazano na sliki 4.3. Skupini *gostujoci profili* smo omogočili skupno rabo s polnimi pravicami za branje in pisanje, kot je prikazano na sliki 4.4. Za večjo zasebnost smo vključili opcijo (ang.



Slika 4.3 Nastavitev varnostnih pravic za skupino gostujoci profili.



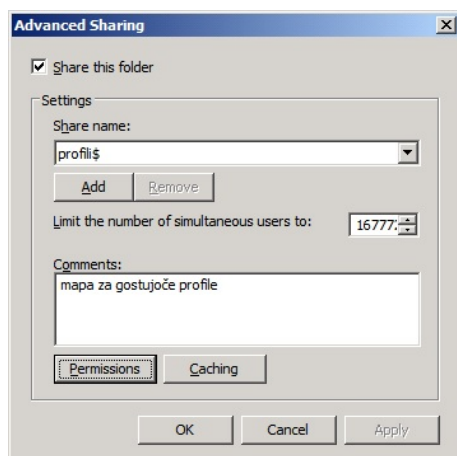
Slika 4.4 Napredna nastavitev pravic za dostop do mape profil\$ v skupni rabi.



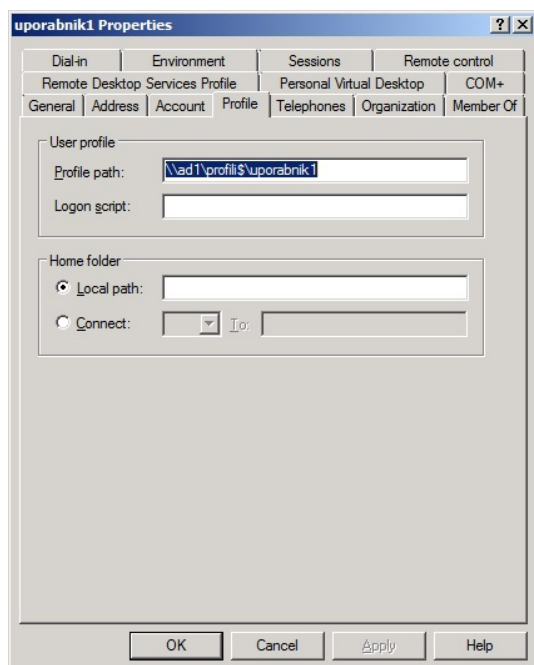
Slika 4.5 Omogočanje Access-based enumeration in izklop razpoložljivosti datotek v času brez povezave.

access-based enumeration), ki poskrbi za to, da uporabnik vidi samo mape nad katerimi ima pravice, ter za potrebe delovanja gostujočih profilov onemogočili razpoložljivost datotek v času brez povezave (ang. *offline settings*) [10], slika 4.5. Priporočljivo je koncu imena dodati znak \$, kot je prikazano na sliki 4.6, ki poskrbi za to, da mapa v skupni rabi ni prosto vidna v Windows raziskovalcu. Za dostop je tako potrebno vpisati točno pot, v našem primeru \\ad1\\profil\$.

V konzoli Active Directory Users and Computers smo kreirali uporabnika in mu v za-
vihu 'Profile' določili novo pot mape profila v skupni rabi na \\ad1\\profil\\%username%,
kot je prikazano na sliki 4.7. Niz %username% se po potrditvi avtomatsko pretvori v
uporabniško ime uporabnika, katerega objekt popravljamo. Uporabniške mape pro-
filov se privzeto kreirajo z ekskluzivnimi pravicami, kar pomeni da do njih nimajo do-
stopa niti administratorji. Zato smo za potrebe testa pripravili nov objekt domenske
politike (ang. *group policy object*) z imenom Omogoci dostop Administratorjem do
gostujocih profilov, ki ob kreiranju uporabniških map doda pravice za dostop tudi
administratorski skupini. V objektu smo omogočili parameter *Add the Administrators
security group to roaming user profiles*, ki se nanaša na delovne postaje in se nahaja v
'Computer Configuration > Policies > Administrative Templates > System User Profiles'.
V produkcijskem okolju je uporaba odvisna od politike podjetja. Če politika to dovoljuje,



Slika 4.6 Dodajanje skrite mape profil\$ v skupno rabo.



Slika 4.7 Nastavitev poti uporabniškega profila objekta uporabnik1 v konzoli Active Directory Users and Computers.

je administracija bistveno lažja, saj mora sicer administrator pri morebitni obnovi ali premiku datotek prevzeti lastništvo nad mapo uporabnikovega profila na strežniku, kar je zamudno in lahko povzroči, da uporabnik zgubi pravice za dostop do svojih datotek.

Ob prvi prijavi uporabnika **uporabnik1** na delovno postajo **pc1** operacijski sistem preveri, če profil obstaja na strežniku. Ker gre za prvo prijavo, profila na strežniku še ni. Na delovni postaji se avtomatsko generira nov profil, na strežniku pa prazna mapa z imenom uporabnik1.v2. Od potrditve vnosa uporabniškega imena in gesla do popolnoma pripravljenega namizja je trajalo 19,96 sekunde. Takoj po uspešni prijavi smo uporabniku **uporabnik1** nastavili profil, kot je opisano v uvodu tega poglavja. Pred odjavo smo preverili mapo uporabnikovega profila na strežniku, ki je bila prazna. Po uspešni odjavi, ki je trajala 22,23 sekunde, se je vsebina map prikazanih na sliki 3.1 iz delovne postaje prenesla na strežnik, z izjemo AppData, kjer se je prenesla le podmapa Roaming. Nato smo se kot **uporabnik1** prijavili na delovno postajo **pc2**. Ker je uporabnikov profil na strežniku že obstajal, se je pričel prenos datotek na delovno postajo. Uporabnik ni mogel pričeti z delom, dokler vsebina profila ni bila v celoti prenesena. Od potrditve vnosa uporabniškega imena in gesla do popolnoma pripravljenega namizja, ki je vsebovalo bližnjice z datotekami ustvarjenimi na **pc1**, je trajalo 38,17 sekunde. Po prijavi smo preverili, če ima uporabnik na delovni postaji **pc2** enak profil, kot na **pc1**. Vsebina profila je bila identična. V mapi 'Moji dokumenti' smo duplicirali 10 naključnih datotek velikosti 10240 KB, tako da je imel uporabnik skupno 1110 datotek, ki so skupaj na disku zasedle 1,18 GB prostora. V 'Windows raziskovalcu' smo nastavili padajoč prikaz glede na velikost datoteke. Nato smo **uporabnika1** odjavili iz delovne postaje **pc2**. Odjava je trajala 188,5 sekunde. Medtem smo lahko na strežniku **ad1** v mapi 'Moji dokumenti' **uporabnika1** spremljali kopiranje datotek v mapo uporabnikovega profila. Ponovno smo se prijavili na delovno postajo **pc1**. Prijava je trajala 10,5 sekunde. Pričakale so nas vse datoteke, ki jih je uporabnik ustvaril med gostovanjem na delovni postaji **pc2** in nastavitve padajočega prikaza v 'Windows raziskovalcu'. Odjava uporabnika je trajala 2,56 sekunde.

Za potrebe testa izpada povezave na oddaljeni lokaciji smo na delovni postaji **pc2** izključili mrežno povezavo. Prijava je bila mogoča in je trajala 38,39 sekunde, uporabljena je bila lokalna kopija profila, v orodni vrstici pa se je prikazalo obvestilo o težavah z roaming profilom. V datoteki test.txt smo spremenili vsebino v '4,3,2,1', zbrisali smo vseh 10 dupliciranih datotek, ki so se premaknile v 'Koš, tako je bilo v mapi 'Moji

dokumenti' spet 1100 naključnih datotek, ki so skupaj zasedle 1,09 GB prostora na disku. Odjava je trajala 4,92 sekunde. Prijavili smo se na delovno postajo **pc1**, prijava je trajala 5,37 sekunde in v datoteki `test.txt` vsebino '1,2,3,4', spremenili v '5,6,7,8' ter se odjavili. Odjava je trajala 2,92 sekunde. Vključili smo mrežno povezavo **pc2** in se prijavi na delovno postajo. Prijava je trajala 11,35 sekunde. Datoteke, ki smo jih v času brez povezave zbrisali, so se nahajale v 'Košu', med tem ko so se v mapo 'Moji dokumenti' presnele iz strežnika, tako da jih je bilo zopet 1110 in so skupaj zasedle 1,09 GB prostora. Enako se je zgodilo z datoteko `test.txt`, ki je sedaj vsebovala niz '5,6,7,8'. Uporabnik je imel tako v mapi 'Moji dokumenti' datoteke, ki jih je med prijavo v času brez povezave zbrisal. Vsebina datoteke `test.txt`, spremenjena v času brez povezave, pa je bila izglubljena brez uporabnikove vednosti. Odjava je trajala 6,89 sekunde.

Test je pokazal, da gostujoči profili uporabnikom omogočajo dostop do svojega profila iz katere koli delovne postaje, ki ima delujočo mrežno povezavo. Ker so podatki shranjeni na centralnem strežniku je možno centralizirano arhiviranje na trakove. Pogojno omogočajo delo oz. dostop do podatkov v primeru začasnega izpada pod določenimi pogoji:

- v primeru, da je uporabnik na delovni postaji že gostoval ima dostop do kopije podatkov, ki je bila ustvarjena ob prejšnjem gostovanju;
- v primeru, da uporabnik na delovni postaji še ni gostoval, nima dostopa do svojih podatkov;

Slabost se je izkazala na primeru, kjer je ob izpadu povezave med prijavo in odjavo, uporabnik trajno izgubil spremembe v datotekah ali cele datoteke brez opozorila. V testnem primeru smo se omejili zgolj na datoteke na namizju in v mojih dokumentih. Na enak način se lahko zgubijo tudi druge nastavitve, ki pa jih uporabniki v praksi redkeje spreminjajo, zato je verjetnost za pojav napake bistveno manjša. Poleg omenjenega je potrebno opozoriti na počasno prijavo in odjavo, ki je odvisna od količine uporabnikovih podatkov, hitrosti linije, obremenitve linije (še posebno v primeru prijave več uporabnikov hkrati) in strežnika. V praksi se lahko zgodi, da uporabnik zaradi neučakanosti ponovno zažene računalnik in s tem povzroči neželeno napako pri sinhronizaciji profila, v najslabšem primeru pa se profil lahko celo poškoduje. Prijava tako ni več mogoča, dokler administrator ne odpravi napak.

4.4 Uporaba preusmeritev map

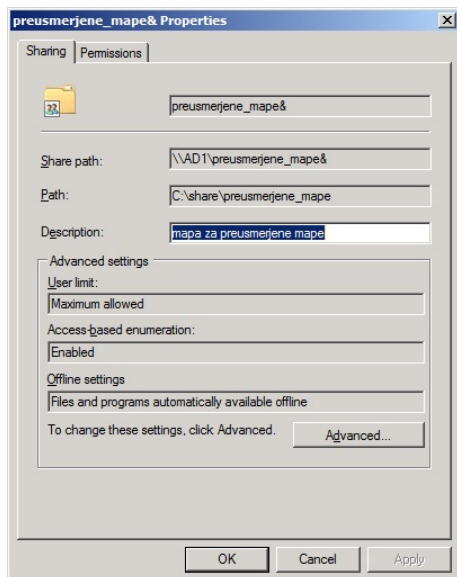
Microsoftova tehnologija preusmeritev map (ang. *folder redirection*), z razliko od gostujočih profilov, omogoča administratorjem preusmeritev posameznih map znotraj uporabniškega profila na drugo lokacijo. Ta je lahko na isti delovni postaji ali na disku strežnika v omrežju. Uporabnik lahko dela s preusmerjenimi dokumenti na enak način, kot da bi se fizično nahajali na njegovi delovni postaji, obenem pa so mu na voljo na vseh delovnih postajah v omrežju. Tehnologijo Microsoft razvija že dalj časa, z vsako novo različico pa uvedejo nekaj izboljšav in sprememb. V Microsoft Windows 7 je podprta preusmeritev naslednjih map:

- AppData/Roaming,
- Contacts,
- Desktop,
- Documents,
- Downloads,
- Favorites,
- Links,
- Music,
- Pictures,
- Saved Games,
- Searches,
- Start Menu,
- Videos.

Spremembo lokacije in posamezne nastavitve se lahko opravi v registru delovne postaje. Na tistih, ki so priključene domeni, se jih nastavi centralizirano prek GPO politike z uporabo konzole za upravljanje skupinske politike (GPMC - *Group Policy Management Console*) [4]. Storitve preusmeritev map deluje v povezavi s tehnologijo Offline File technology, znano kot pomnjenje na klientovi strani (CSC - *Client Side Caching*), ki je v operacijskem sistemu Microsoft Windows 7 privzeto omogočena. Deluje v načinu online in offline. V online načinu do datotek dostopa s hitrostjo kot jo omogočata mrežna povezava in strežnik. V offline načinu, torej v primeru nedosegljivosti ali počasne povezave, operacijski sistem uporablja kopijo, ki se nahaja na lokalnem disku na področju %systemroot%\CSC v binarni obliki. V Windows 7 in Windows Server 2008R2 Offline File technology omogoča [12]:

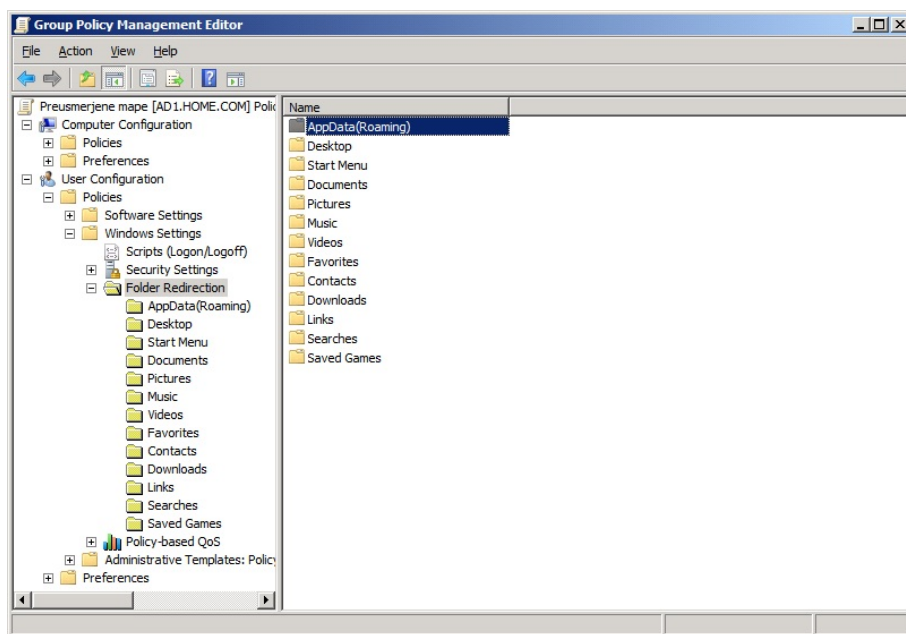
- Hitro prvo prijavo (ang. *fast first logon*): V starejših različicah je moral uporabnik ob prvi prijavi počakati, da so se njegovi dokumenti prek omrežja prenesli na strežnik. Z uporabo hitre prijave se dokumenti lokalno premaknejo v pomnilnik offline datotek (ang. *Offline Files cache*), sinhronizacija oz. prenos na strežnik se opravi v ozadju, uporabnik pa lahko med tem nemoteno opravlja svoje delo.
- Uporabo offline načina s sinhronizacijo v ozadju (ang. *usually offline support with background sync*), ki v primeru počasne povezave, izpada ali večje obremenjenosti strežnika, omogoča uporabnikom nemoteno delo: Uporabnikom ni potrebno skrbeti za ročno sinhronizacijo, tako kot v starejših različicah Windows, saj se izvede avtomatsko, takrat ko je povezava na voljo. Administrator lahko nastavi intervale in čase med katerimi sinhronizacija ni aktivna.
- Uporabo seznama izjem (ang. *exclusion list*), ki je namenjen manjši obremenitvi omrežja in diskovnega prostora na strežniku: Administrator lahko v skladu s politiko podjetja iz sinhronizacije izloči datoteke, ki za podjetje niso pomembne in tako med sinhronizacijo ne obremenjujejo omrežja ter po nepotrebnem zasedajo dragega prostora na strežniku.
- Transparentno pomnjenje (ang. *transparent caching*) optimizira porabo pasovne širine na omrežju. Ob prvem dostopu do datoteke v skupni rabi, se le ta shrani na lokalni disk. Ob vsakem naslednjem dostopu se uporabi lokalno shranjena kopija, mehanizem pa preveri, če je datoteka enake verzije kot tista na strežniku. Če uporabnik naredi kakšno spremembo, se le ta shrani lokalno in na strežnik. V primeru nedostopnosti strežnika uporabnik ne more dostopati do datoteke shranjene na lokalnem disku. Transparentno pomnjenje ni vključeno kot privzeto. Administrator ga mora vključiti ročno z uporabo GPO.

Za preizkus rešitve smo na testnem virtualnem domenskem strežniku **ad1** kreirali uporabnika z uporabniškim imenom **uporabnik2** ter varnostno skupino *preusmerjene mape*, ki jo bomo potrebovali za nastavitve varnostnih pravic in dodeljevanja skupne rabe. Na trdem disku strežnika **ad1** smo kreirali mapo z imenom **preusmerjene_mape**, ki bo služila za shranjevanje datotek uporabnikovega profila. V naprednih varnostnih nastavitvah smo izključili dedovanje, nastavili varnostne pravice za dostop, dali mapo v skupno in dodelili pravice enako kot pri uporabi gostujočih profilov. Razlika je v nastavitvi razpoložljivosti datotek v času brez povezave, ki smo jo za pravilno delovanje preusmer-

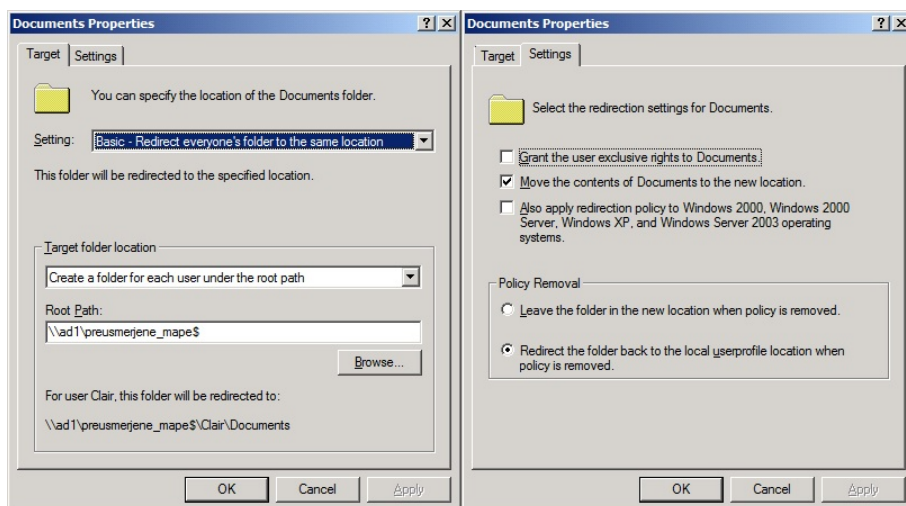


Slika 4.8 Omogočanje Access-based enumeration in vklop razpoložljivosti datotek v času brez povezave.

jenih map vključili, kot je prikazano na sliki 4.8. Na strežniku **ad1** smo ustvarili nov GPO objekt **Preusmerjene mape**, v katerem smo nastavili parametre User Configuration\Policies\Windows Settings\Folder Redirection, za preusmeritev posameznih map, ki so prikazane na sliki 4.9. Vsaki mapi posebej smo v zavihku 'Target' nastavili ustrezno pot (z izjemo map 'Pictures', 'Music' in 'Videos', kjer smo izbrali, da sledijo mapi 'Documents'), v zavihku 'Settings' pa nastavili, da uporabnikove mape niso kreirane z ekskluzivnimi pravicam (ang. *grant the user exclusive rights to Documents*), da se vsebina premakne na v zavihku 'Target' izbrano lokacijo (ang. *move the contents of Documents to the new location*) in da se v primeru izklopa politike mape preusmerijo nazaj k lokalnem profilu (ang. *redirect the folder back to the local userprofile ocation when policy is removed*). Slika 4.10 prikazuje nastavitve obeh zavihkov mape 'Documents'. Ob prvi prijavi uporabnika **uporabnik2** na delovno postajo **pc1** se je naložilo privzeto namizje. Od potrditve vnosa uporabniškega imena in gesla do popolnoma pripravljenega namizja je trajalo 18,38 sekunde. Ker pravila GPO privzeto začnejo veljati po 90 minutah z naključnim zamikom 0 do 30 minut [7], smo po uspešni prijavi v ukazni vrstici (ang. *command prompt*) zagnali ukaz 'gpupdate/force'. Po obvezni odjavi in prijavi uporabnika smo s tem dosegli takojšnjo veljavo pravila **preusmerjene_mape**. Odjava je trajala 1,61 sekunde, ponovna prijava, ki je v bistvu prva z uporabo preusmerjenih map pa



Slika 4.9 Konzola za nastavitve GPO, ki prikazuje parametre za nastavitve preusmeritev map. Z desnim klikom na posamezno mapo je na voljo več možnosti.

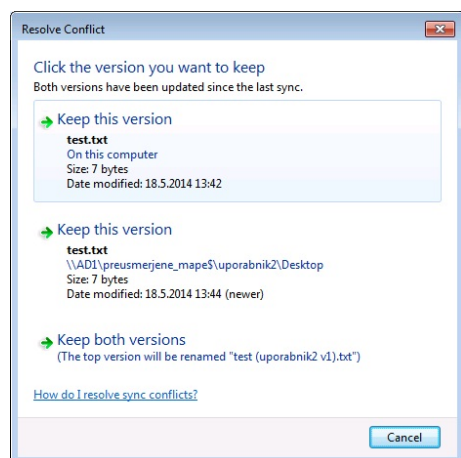


Slika 4.10 Prikaz zavihka 'Target' in 'Settings' za nastavitve preusmeritve na mapi 'Documents'.

75,4 sekunde. Uporabniku **uporabnik2** smo nastavili profil, kot je opisano v uvodu tega poglavja. Pred odjavo smo preverili mapo uporabnikovega profila na strežniku, ki je že vsebovala vse datoteke preusmerjene iz uporabniškega profila. Odjava je trajala 6,46 sekunde.

Nato smo se kot **uporabnik2** prijavili na delovno postajo **pc2**. Uporabnik ni mogel pričeti z delom, dokler vsebina map, obvezna za prikaz namizja ni bila prenesena iz strežnika. Od potrditve vnosa uporabniškega imena in gesla do popolnoma pripravljenega namizja, ki je vsebovalo bližnjice z datotekami, ustvarjenimi na **pc1** je trajalo 27,24 sekunde. Po prijavi smo preverili, če ima uporabnik na delovni postaji **pc2** enak profil kot na **pc1**. Vsebina dokumentov v mapi 'Moji dokumenti' in namizja je bila identična, ozadje namizja in bližnjice na namizju pa niso bile razporejene enako, kot na delovni postaji **pc1**. Nastavitve orodne vrstice in brskalnika Internet Explorer vključno z digitalnim potrdilom se niso prenesle. V mapi 'Moji dokumenti' smo duplicirali 10 naključnih datotek velikosti 10240 KB, tako da je imel uporabnik skupno 1110 datotek, ki so skupaj na disku zasedle 1,18 GB prostora. Glede na hitrost duplikacije 602 KB/sekundo smo sklepali, da se izvaja z uporabo mrežne povezave na strežniku **ad1**. V Windows raziskovalcu smo nastavili padajoč prikaz glede na velikost datoteke. Nato smo **uporabnika2** odjavili iz delovne postaje **pc2**. Odjava je trajala 7,13 sekunde. Ponovno smo se prijavili na delovno postajo **pc1**. Prijava je trajala 9,5 sekunde. Pričakale so nas vse datoteke, ki jih je uporabnik ustvaril med gostovanjem na delovni postaji **pc2**, nastavitve padajočega prikaza v 'Windows raziskovalcu' pa se ni ohranila. Odjava uporabnika je trajala 2,45 sekunde.

Za potrebe testa izpada povezave na oddaljeni lokaciji smo na delovni postaji **pc2** izključili mrežno povezavo. Prijava je bila mogoča in je trajala 38,32 sekunde. V datoteki **test.txt** smo spremenili vsebino v '4,3,2,1', zbrisali smo vseh 10 dupliciranih datotek, ki so se premaknile v 'Koš'. Tako je bilo v mapi 'Moji dokumenti' spet 1100 naključnih datotek, ki so skupaj zasedle 1,09 GB prostora na disku. Odjava je trajala 2,12 sekunde. Prijavili smo se na delovno postajo **pc1**. Prijava je trajala 6,21 sekunde in v datoteki smo **test.txt** vsebino '1,2,3,4', spremenili v '5,6,7,8' ter se odjavili. Odjava je trajala 1,84 sekunde. Vključili smo mrežno povezavo **pc2** in se prijavili na delovno postajo. Prijava je trajala 8,76 sekunde. Datoteke, ki smo jih v času brez povezave zbrisali, so se nahajale v 'Košu', med tem ko jih v mapi 'Moji dokumenti' ni bilo več, tako da jih je bilo zopet 1110 in so skupaj zasedle 1,09 GB prostora. Datoteka 'test.txt' je vsebovala niz '4,3,2,1', ki ga



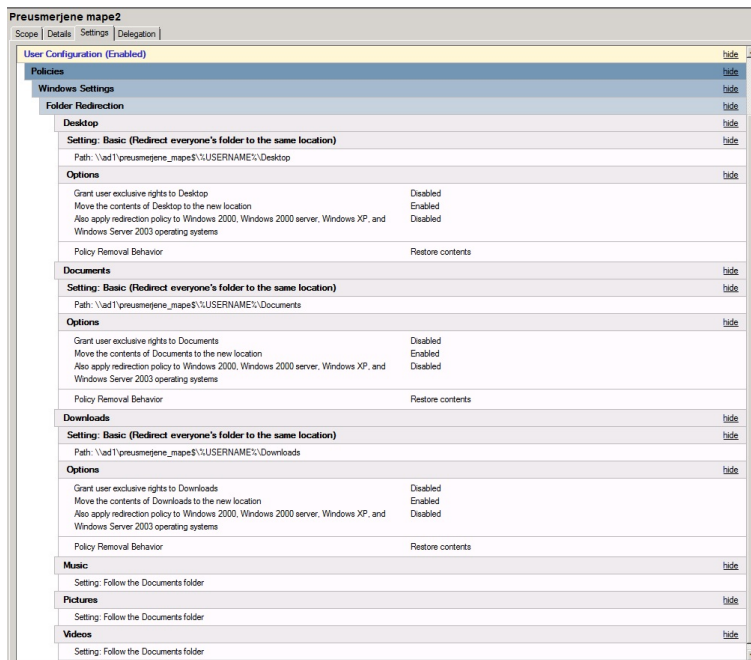
Slika 4.11 Izbira ustrezne verzije datoteke.

je uporabnik vnesel v času brez povezave. V orodni vrstici se je prikazal oblaček 'Sync Center', ki je sporočal, da je prišlo do 27 konfliktov [1]. Uporabniku je za vsak konflikt posebej ponudil možnost razrešitve, kjer je imel uporabnik možnost obdržati trenutno datoteko, izbrati tisto iz strežnika ali pa obe, kot je prikazano na sliki 4.11. Med konflikti se je nahajala datoteka test.txt, ki je sedaj vsebovala niz '5,6,7,8'. Uporabnik je imel tako v mapi 'Moji dokumenti' datoteke, ki jih je med delom v času brez povezave zbrisal. Odjava je trajala 6,89 sekunde.

Test je pokazal, da preusmeritev map uporabniku zagotavlja dostop do datotek, ki se nahajajo v omenjenih mapah. Prinaša prednost v primerjavi z uporabo gostujočih profilov, saj količina podatkov, hitrost in obremenjenost povezave ter strežnika zaradi izvajanja v ozadju nimajo bistvenega vpliva na dolžino prijave in odjave. V primeru vzpostavitve povezave med tem, ko je uporabnik prijavljen, se dokumenti prenesejo v ozadju. Slaba stran rešitve je, da v sinhronizacijo v našem primeru niso vključene nastavitve programov, ozadje namizja, razporeditev bližnjic na namizju, bližnjice orodne vrstice in digitalna potrdila v internetnem brskalniku.

4.5 Uporaba gostujočih profilov s preusmerjenimi mapami

Z uporabo kombinacije gostujočih profilov in preusmerjenih map se na račun umika velikih uporabnikovih datotek iz uporabnikovega profila izognemo počasnim prijavam in odjavam, hkrati pa omogočimo, da imajo uporabniki na vseh delovnih postajah poleg svojih dokumentov tudi vse nastavitve delovnega okolja. Rešitev uporabnikom zagota-



Slika 4.12 Prikaz nastavitve GPO objekta Preusmerjene mape 2 v konzoli Group Policy Management.

vlja enako uporabniško izkušnjo na vseh delovnih postajah v podjetju in sinhronizacijo posameznih map v ozadju.

Za preizkus rešitve smo kreirali novega uporabnika z imenom **uporabnik3**, ki smo ga dodali v varnostni skupini kreirani v podpoglavju 4.3 in 4.4:

- **preusmerjene_mape**: za dostop do mape v skupni rabi, namenjene preusmeritvi datotek;
- **profili**: za dostop do mape v skupni rabi, namenjene preusmeritvi preostalega dela uporabnikovega profila;

Za uporabo gostujočih profilov smo uporabniku **uporabnik3** v konzoli Active Directory Users and Computers v zavihku 'Profile' nastavili pot mape profila v skupni rabi na \\ad1\profili\%username%. Mape smo preusmerili z na novo kreiranim GPO objektom **Preusmerjene mape 2**, kjer smo preusmerili pot samo mapam Namizje, Prenosi in 'Moji dokumenti', vključno s podmapami 'Slike', 'Glasba' in 'Video', kot je prikazano na sliki 4.12. Ker je profil uporabnika **uporabnik3** povezan z uporabo GPO, smo morali ob prvi prijavi na delovno postajo **pc1**, ki je trajala 14,5 sekunde, za takojšnjo uveljavitev politike v ukazni vrstici zagnati ukaz 'gpupdate/force'. Odjava je trajala 1,44 sekunde,

ponovna prijava pa 35,86 sekunde. Uporabniški profil uporabnika **uporabnik3** je bil s tem pripravljen za nastavitve namizja, Internet Explorerja in pripravo datotek v mapi 'Moji dokumenti'. Pred odjavo smo preverili mapo uporabnikovega profila in mapo preusmerjenih map na strežniku **ad1**. Uporabnikov profil je bil prazen, mapa preusmerjenih map pa je vsebovala nove datoteke. Odjava je trajala 1,55 sekunde.

Prijava uporabnika **uporabnik3** na delovno postajo **pc2** je trajala 12,63 sekunde. Vsebina mape 'Moji dokumenti', ozadje namizja, bližnjice na namizju, bližnjice v orodni vrstici in digitalno potrdilo v spletnem brskalniku, vse je bilo identično kot smo nastavili na delovni postaji **pc1**. V mapi 'Moji dokumenti' smo duplicirali 10 naključnih datotek velikosti 10240 KB, tako da je imel uporabnik skupno 1110 datotek, ki so skupaj na disku zasedle 1,18 GB prostora. V 'Windows raziskovalcu' smo nastavili padajoč prikaz glede na velikost datoteke. Nato smo **uporabnika3** odjavili iz delovne postaje **pc2**. Odjava je trajala 4,42 sekunde. Ponovno smo se prijavili na delovno postajo **pc1**. Prijava je trajala 7,9 sekunde. Pričakale so nas vse datoteke, ki jih je uporabnik ustvaril med gostovanjem na delovni postaji **pc2**, nastavev padajočega prikaza v 'Windows raziskovalcu' pa se je ohranila. Odjava uporabnika je trajala 1,72 sekunde.

Za potrebe testa izpada povezave na oddaljeni lokaciji, smo na delovni postaji **pc2** izključili mrežno povezavo. Prijava je bila mogoča in je trajala 38,32 sekunde. V datoteki **test.txt** smo spremenili vsebino v '4,3,2,1' in zbrisali vseh 10 dupliciranih datotek, ki so se premaknile v 'Koš'. Tako je bilo v mapi 'Moji dokumenti' spet 1100 naključnih datotek, ki so skupaj zasedle 1,09 GB prostora na disku. Odjava je trajala 1,12 sekunde. Prijavili smo se na delovno postajo **pc1**, prijava je trajala 9,84 sekunde in v datoteki **test.txt** vsebino '1,2,3,4', spremenili v '5,6,7,8' ter se odjavili. Odjava je trajala 2,32 sekunde. Vključili smo mrežno povezavo **pc2** in se prijavili na delovno postajo. Prijava je trajala 10,51 sekunde. Datoteke, ki smo jih v času brez povezave zbrisali, so se nahajale v 'Košu', med tem ko jih v mapi 'Moji dokumenti' ni bilo več, tako da jih je bilo zopet 1110 in so skupaj zasedle 1,09 GB prostora. Datoteka 'test.txt' je vsebovala niz '4,3,2,1', ki ga je uporabnik vnesel v času brez povezave. V orodni vrstici se je prikazal oblaček 'Sync Center', ki je sporočal, da je prišlo do enega konflikta. Uporabnik je lahko izbral ali bo obdržal trenutno datoteko, izbral verzijo iz strežnika, ali pa obe.

Enako se je zgodilo z datoteko **test.txt**, ki je sedaj vsebovala niz '5,6,7,8'. Uporabnik je imel tako v mapi 'Moji dokumenti' datoteke, ki jih je med delom v času brez povezave zbrisal. Vsebina datoteke **test.txt**, spremenjena v času brez povezave, pa je bila

izgubljena brez uporabnikove vednosti. Odjava je trajala 4,27 sekunde.

Kombinacija gostujočih profilov in preusmeritve map, v katere uporabnik shranjuje svoje datoteke, zagotavlja dostop do datotek neodvisno od delovne postaje na katero se prijavi. Prinaša prednost v primerjavi z uporabo gostujočih profilov, saj količina podatkov, hitrost in obremenjenost povezave ter strežnika zaradi izvajanja v ozadju nimajo bistvenega vpliva na dolžino prijave in odjave. Gostujoči profili poskrbijo za sinhronizacijo nastavitve programov, ozadje namizja, razporeditev bližnjic na namizju, bližnjice orodne vrstice in digitalnih potrdil v internetnem brskalniku. V primeru vzpostavitve povezave med tem, ko je uporabnik prijavljen, se dokumenti prenesejo v ozadju, nastavitve programov pa ob ponovni prijavi.

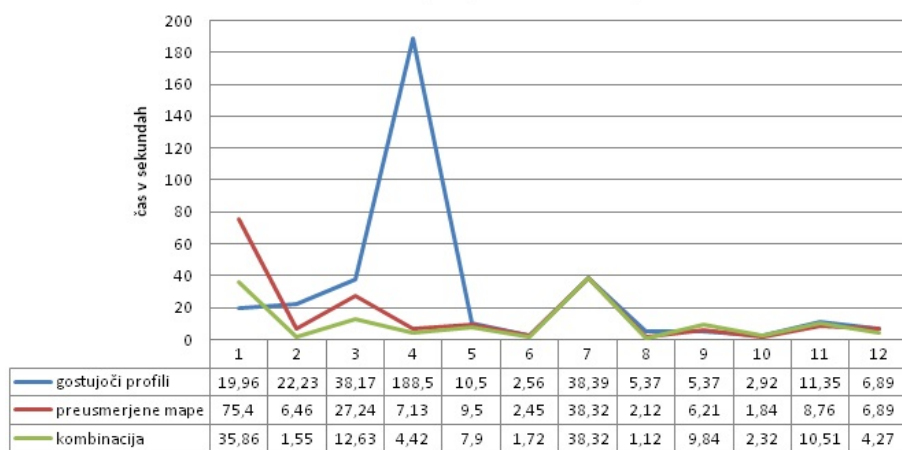
4.6 Primerjava in problemi rešitev

Rešitve predstavljene v podpoglavjih 4.3, 4.4 in 4.5 z izjemo preusmeritev map, ki uporabniku ne zagotavlja nastavitve posameznih programov, uporabe po uporabnikovih željah prilagojenega namizja in prenosa digitalnega potrdila, izpolnjujejo pogoje, ki smo jih zastavili v poglavju 2. Katerokoli je mogoče uporabiti na obstoječi infrastrukturi brez dodatnih stroškov, vse omogočajo shranjevanje uporabnikovih podatkov vključenih v profil na centralni strežnik za potrebe izdelave varnostnih kopij.

Za lažjo primerjavo časa potrebnega za prijavo in odjavo med posameznimi rešitvami smo čase iz pridobljene na testnih primerih predstavili na grafikonu 4.13. Čase vseh prijav in odjav s posameznimi rešitvami smo sešteli ter izračunali povprečen čas. Podatki so prikazani na grafikonu 4.14. V praksi je več primerov, kjer se uporabnik prijavlja in odjavlja na isti delovni postaji, oziroma na postaje kjer je nekoč že bil prijavljen, kot pa prvih prijav na za uporabnika novo delovno postajo. Zaradi slednjega rezultati na grafikonih ne prikazujejo povsem realne slike, je pa jasno razvidna prednost rešitve z uporabo gostujočih profilov in preusmerjenih map.

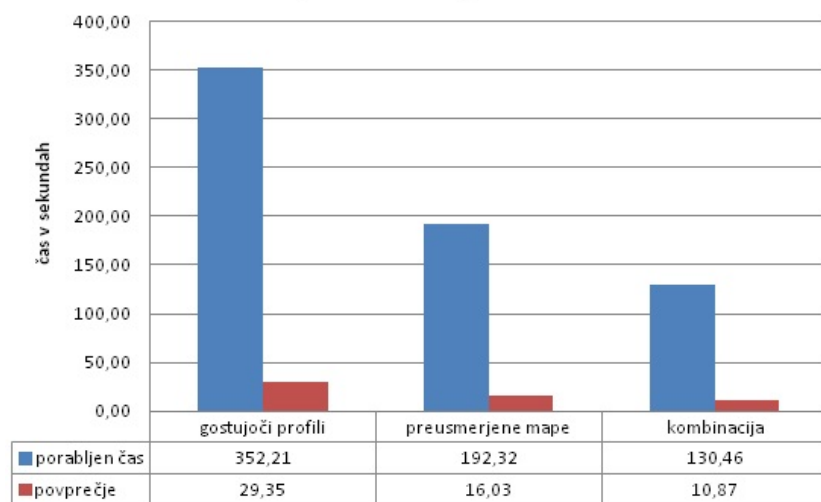
Vsem rešitvam je skupno, da ne omogočajo prve prijave v primeru izpada povezave s centralno lokacijo. To bi bilo možno rešiti s postavitvijo dodatnega datotečnega strežnika v vsaki izmed poslovalnic, na katerem bi se nahajali profili vseh uporabnikov. Profili bi se med strežnikom na centralni lokaciji in tistim v poslovalnici sinhronizirali v ozadju z uporabo distribuiranega datotečnega sistema (DFS - *distributed file system*) [13], uporabniku pa bi se ob prijavi na delovno postajo naložil profil iz strežnika v poslovalnici. Na

Prikaz časa porabljenega pri testiranju prijav in odjav z različnimi rešitvami po posameznih primerih



Slika 4.13 Grafikon prikazuje primerjavo časov prijav in odjav pri posameznih rešitvah na testnih primerih.

Prikaz skupno porabljenega in povprečnega časa pri testiranju rešitev



Slika 4.14 Grafikon prikazuje skupno porabljen čas za vse prijave in odjave v testnih primerih ter povprečni čas za odjavo ali prijavo.

ta način bi zagotovili možnost prve prijave ob izpadu povezave, obenem pa bi se izognili vplivu počasne povezave na dolžino prijave in odjave. Potreben bi bil nakup strežnikov za vse poslovalnice, vsak izmed njih pa bi moral imeti na trdem disku dovolj prostora za profile vseh uporabnikov.

Problem počasne prijave in odjave je rešljiv z uporabo tehnologije BranchCache [3], ki lahko deluje na distribuiran (ang. *distributed cache mode*) in gostujoč način (ang. *hosted cache mode*). Distribuiran način omogoča shranjevanje podatkov na lokalnem disku do 50 računalnikom v posamezni poslovalnici. Na ta način bi se uporabniku, ki se seli lokalno po poslovalnici skrajšal čas prijave in odjave, saj bi se profil naložil prek hitrega lokalnega omrežja, brez omejitve, ki jih prinaša počasna povezave s centralno lokacijo.

S časom postajajo profili vse bolj prostorsko potratni, uporabnikovi podatki ne povzročajo večjih težav, saj zaradi uporabe preusmerjenih map ne vplivajo bistveno na dolžino prijave in odjave. Problem se lahko pojavi v mapi **AppData**, kjer so shranjene začasne datoteke, zgodovina brskanja in piškotki brskalnika Internet Explorer. Poleg tega nekatere slabo napisane aplikacije vanjo shranjujejo svoje začasne datoteke. Datoteke so ponavadi manjše in se jih lahko nabere tudi več kot nekaj 10.000. Temu se lahko izognemo tako, da ustvarimo GPO pravilo, ki omeji prostor namenjen začasnim datotekam, skrajša čas shranjevanja zgodovine brskanja, ter s periodičnim ročnim brisanjem začasnih datotek v mapi **AppData**.

Ker deli uporabnikovega profila po njegovi odjavi ostanejo na trdem disku delovne postaje, s časom na tistih postajah, na katerih je gostovalo veliko uporabnikov zmanjka prostora na trdem disku. Nekateri od uporabnikov lahko vmes zapustijo podjetje. Administratorji ponavadi odstranijo njihove datoteke iz datotečnega strežnika, zelo težko pa ugotovijo na katerih delovnih postajah so gostovali v času zaposlitve. Taki profili po nepotrebnem zasedajo prostor na delovnih postajah. Zato je priporočljiva uporaba GPO pravila, ki se nahaja v Computer Configuration\Policies\Administrative Templates\System\User Profiles in se imenuje **Delete user profiles older than a specified number of days on system restart**. Pravilo poskrbi, da se ob ponovnem zagonu delovne postaje iz trdega diska odstranijo datoteke s profili starejšimi od naprimer 90 dni. Profil tako še zmeraj ostane na datotečenem strežniku, zbršejo se le datoteke na posameznih delovnih postajah, na katerih uporabnik dalj časa ni gostoval.

V primeru, da se uporabnik po končanem delu pozabi odjaviti iz delovne postaje

in nadaljuje delo s prijavo na drugo delovno postajo, lahko na delu profila za katerega skrbijo gostujoči profil pride do izgube podatkov. Kot je opisano v poglavju 4.3 se podatki shranijo na strežnik ob uporabnikovi odjavi. V tem primeru podatki iz prve delovne postaje niso shranjeni, med tem ko uporabnik na drugi delovni postaji ustvari nove, ki se ob odjavi shranijo na strežnik. Kasneje se ob odjavi iz delovne postaje kjer je uporabnik delal prej, podatki, ki so nastali kasneje, prepisejo s starimi. Microsoft zaenkrat ne omogoča načina za nadzor nad prijavami na več delovnih postaj naenkrat. Obstajajo alternativne rešitve, ki pa imajo določene pomanjkljivosti.

Administratorji v podjetju morajo poskrbeti, da so na vseh računalnikih naložene iste verzije programov, saj v nasprotnem primeru ni zagotovljeno pravilno shranjevanje nastavitvev aplikaciji. Lahko se tudi zgodi, da uporabnik ustvari bližnjico do posamezne aplikacije, ki zaradi drugačne poti ali druge verzije aplikacije ne bo delovala.

Microsoft je z novejšimi verzijami operacijskega sistema spreminjal zgradbo profila. Tako uporabniški profil, kreiran ob prijavi na delovni postaji na kateri je nameščen operacijski sistem Windows XP, ni kompatibilen s tistimi z Windows 7, ki je le enosmerno kompatibilen z Windows 8 in Windows 8.1 [11]. To pomeni, da uporabniški profil kreiran na računalniku z Windows 7 ob prijavi na delovno postajo z Windows 8 deluje. Težava nastane, ko se uporabnik ponovno prijavi na delovno postajo z Windows 7, saj profil vsebuje za Windows 7 neznane spremembe, ki so bile shranjene v Windows 8. Problem lahko odpravimo tako, da imamo ločene profile, odvisne od operacijskega sistema. V tem primeru uporabniške nastavitve ne migrirajo med različnimi verzijami Windows, omogočen pa je dostop do preusmerjenih map. Obstajajo tudi neodvisne programske rešitve, ki rešujejo probleme s kompatibilnostjo profilov. Ena izmed njih je ProfileUnity™, dostopna na spletni strani <http://www.liquidwarelabs.com/products/profileunity>.

Z ustrezno zasnovanim informacijskim sistemom in ozaveščenimi uporabniki se lahko večini problemov deloma ali v celoti izognemo.

5 Sklepne ugotovitve

Problem uporabe po lastnih potrebah prilagojenega uporabniškega profila in svojih datotek na različnih računalnikih je z uporabo tehnologij, ki so na voljo v Microsoftovem okolju, na prvi pogled preprosto rešljiv.

Rešitev gostujočih profilov, preusmerjenih map in ustrezne kombinacije obeh rešitev skupaj smo časovno ovrednotili v virtualnem okolju na primerih, do katerih pogosto pride v praksi. Gostujoči profili za podjetje zaradi časovno potratnih prijav in odjav iz sistema niso primerni. Prikazali smo primer, v katerem pride do izgube uporabnikovih podatkov, ne da bi uporabnik za to vedel. Uporaba preusmerjenih map zagotavlja krajše čase prijav in odjav, uporabniku pa ne omogoča uporabe celega profila, pač pa samo datoteke v določenih mapah. Do izgube podatkov brez uporabnikove vednosti ne more priti, saj je v primeru napak pri sinhronizaciji o tem obveščen in lahko izbira med verzijo na strežniku in tisto na delovni postaji.

Kot najbolj optimalna se je izkazala kombinacija gostujočih profilov in preusmerjenih map, kjer storitev preusmerjenih map poskrbi za premik velikih uporabnikovih datotek iz profila, zagotavlja sledenje napakam pri sinhronizaciji, gostujoči profili pa poskrbijo za

ostale nastavitve.

Med nastajanjem diplomskega dela je bila v podjetju rešitev uporabljena v dveh različicah. Uporabniki, ki se selijo med delovnimi postajami, uporabljajo gostujoče profile, tisti, ki opravljajo delo na točno določenih delovnih postajah in nimajo potrebe po selitvi, pa zaradi centraliziranega varovanja zgolj preusmeritev mape 'Moji dokumenti'. Zaradi dolgih časov prijav in odjav ter dejstva, da uporabniki, ki uporabljajo preusmerjene mape ob okvari računalnika izgubijo nastavitve profila, bomo na podlagi rezultatov diplomskega dela v kratkem za selitev uporabniških profilov uporabili kombinacijo rešitev gostujočih profilov in preusmerjenih map.

Implementacija rešitve bo optimizirala delovni proces, saj bodo uporabniki porabili manj časa za nepotrebno čakanje pri nalaganju uporabniškega profila, bistveno se bo zmanjšala možnost izgube podatkov, zagotovljeno bo centralizirano izvajanje varnostnih kopij celotnih profilov vseh uporabnikov, poleg naštetega pa bo v primeru okvare trdega diska zagotovljeno nemoteno delo zgolj s prijavo na novo delovno postajo.

LITERATURA

- [1] J. Boyce, Windows 7 Bible, Wiley Publishing, Inc., Indianapolis, 2009.
- [2] L. Bronze, How to setup and configure a domain controller on windows server 2008 r2 (May 2014).
url: <https://support.cloudshare.com/hc/en-us/articles/200701095-How-to-setup-and-configure-a-Domain-Controller-on-Windows-Server-2008-R2>
- [3] R. Charlie, D. Craig, Introducing Windows Server 2008 R2, Microsoft Press, Washington, 2010.
- [4] R. R. King, Mastering Active Directory for Windows Server 2003, Sybex Inc, Alameda, 2003.
- [5] MSDN.Microsoft, About user profiles (May 2014).
url: [http://msdn.microsoft.com/en-us/library/windows/desktop/bb776892\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/bb776892(v=vs.85).aspx)
- [6] MSDN.Microsoft, Roaming user profiles (May 2014).
url: [http://msdn.microsoft.com/en-us/library/windows/desktop/bb776897\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/bb776897(v=vs.85).aspx)
- [7] MSDN.Microsoft, Group policy refresh interval for users (May 2014).
url: <http://msdn.microsoft.com/en-us/library/ms812018.aspx>
- [8] NetworkAdminKB.com, The golden rules of permissions administration (May 2014).
url: <http://networkadminkb.com/KB/a5/the-golden-rules-of-permissions-administration.aspx>
- [9] C. Nigel, M. Alvin, L. Michel, F. Damian, Microsoft System Center, Building a Virtualized Network Solution, Microsoft Press, Washington, 2014.

- [10] Support.Microsoft, the cache option for offline files must be disabled on roaming user profile shares (May 2014).
url: <http://support.microsoft.com/kb/287566>
- [11] Support.Microsoft, Incompatibility between windows 8.1 roaming user profiles and those in earlier versions of windows (May 2014).
url: <http://support.microsoft.com/kb/2890783>
- [12] Technet.Microsoft, Configuring new offline files features for windows 7 computers step-by-step guide (2010).
url: [http://technet.microsoft.com/en-us/library/ff633429\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/ff633429(v=ws.10).aspx)
- [13] Technet.Microsoft, Distributed file system (2014).
url: [http://technet.microsoft.com/en-us/library/cc753479\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc753479(v=ws.10).aspx)
- [14] www.soft.tahionic.com, Free disk tools software (May 2014).
url: <http://www.soft.tahionic.com/download-file-generator/>